REMARKS

The present application was filed on February 12, 2001 with claims 1-18. Claims 1-18 are currently pending in the application. Claims 1, 17 and 18 are the independent claims.

In the present Office Action, claims 1-18 are rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,867,578 to Brickell et al. (hereinafter "Brickell"). Applicants respectfully traverse this rejection and ask for reconsideration based on the following remarks.

Applicants initially note that the Manual of Patent Examination, Eighth Edition, August 2001 (MPEP) §2131 specifies that a given claim is anticipated "only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference," citing Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, MPEP §2131 indicates that the cited reference must show the "identical invention . . . in as complete detail as is contained in the . . . claim," citing Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Independent claim 1 is as follows:

> A method for encrypting a message to be transmitted over a network, wherein the method comprises the steps of:
>
> encrypting the message for transmission over the network, the resulting encrypted message having associated therewith a proof of correctness indicating that the message is of a type that allows decryption by one or more escrow authorities; and
>
> transmitting the encrypted message through the network to a recipient, wherein in traversing the network the proof of correctness associated with the encrypted message is checked by at least one module of a server of the network.

In formulating the §102(b) rejection of this claim, the Examiner argues that the elements beginning with the words "encrypting" and "transmitting" are taught by Brickell in col. 6, line 57 through col. 7, line 15 (Office Action, p. 3). Applicants respectfully disagree. The aforementioned portion of Brickell states:

> In practice it is contemplated that users will also encrypt messages using a symmetric key encryption system. The sender, u, will encrypt a message using a public encryption key (E_u) of the intended recipient, and the recipient will decrypt the message using its corresponding private decryption key (D_u). Analogous to operation of signature/verification keys, messages encrypted using a public encryption key (E_u) can only be decrypted with a corresponding private decryption key (D_u).
>
> As will become readily apparent to one skilled in the art, the foregoing RCA 20 can be used to certify encryption keys in the same manner as is described herein for certifying verification keys. Each user holds its signature key (S_u) and decryption key (D_u) in secret, while allowing distribution and certification of the corresponding verification key (V_u) and encryption key (E_u). It will be appreciated that the security and assurance provided by the user's signature and/or encryption relies in part on the security provided by the signatures of the hierarchy of certifying authorities. Security of signatures relies, in turn, primarily on the cryptographic strength of the signature scheme and on the safety of the private signature keys. It will therefore be appreciated that a compromise of the RCA signature key (also called the "root" key) would destroy the security of the entire system. The root key thus becomes a high-value target for attack by criminals, foreign agents, and hackers.

Applicants submit that one skilled in the art will immediately recognize that this portion of Brickell fails to describe all the elements of claim 1. For instance, Brickell does not describe the use of a "proof of correctness" to indicate "that the message is of a type that allows decryption by one or more escrow authorities" (Specification, p. 2, lines 14-15). Nor does Brickell describe the checking of the "proof of correctness" as the message traverses a network. As a result, Brickell fails to describe each and every element of claim 1, and, therefore, fails to anticipate claim 1 under §102(b).

Examiner also argues that the "proof of correctness" in the present invention is equivalent to Brickell's method for verifying digital signatures (Office action, p. 2). Brickell at col. 3, lines 58-65, explains such method as follows:

> [A] signature certificate for a user is obtained from a certifying authority at a first tier of the hierarchical digital signature system. The signature certificate from the first tier certifying authority is then presented to a higher tier certifying authority which issues a certificate authenticating the signature of the first tier certifying authority. The user then presents a verifier with the authenticating certificate of the higher tier certifying authority.

Applicants submit that one skilled in the art will immediately recognize that Brickell's method for verification of digital signatures and verification of digital signatures in general differ from the claimed "proof of correctness" because, unlike "proof of correctness," such verification schemes fail to associate with an encrypted message an indication as to whether a message can be decrypted by escrow authorities. In addition, the "proof of correctness," by being subject to a check by at least one module of a server of the network, ensures that only valid encryption keys can be used to encrypt a message. See Specification, p. 8, lines 17-28. In contrast to Brickell's method for verification of digital signatures, the invention thus provides immunity against the "sign-the-new-public-key" attack that is described in the Specification, p. 2, lines 1-8.

Dependent claims 2-16 are believed allowable for at least the reasons identified above with regard to claim 1. Moreover, the Examiner states that independent claims 17 and 18 are rejected "along the same rationale" as claim 1 (Office Action, p. 6). Applicants, therefore, also respectfully submit that independent claims 17 and 18 are in condition for allowance for at least the reasons set forth above with respect to claim 1.

Accordingly, Applicants believe that claims 1-18 are in condition for allowance and respectfully request the withdrawal of the §102(b) rejection.

As noted above, a Notice of Appeal is submitted concurrently with this response.

Respectfully submitted,

Joseph B. Ryan

Date: May 31, 2005

Joseph B. Ryan
Attorney for Applicant(s)
Reg. No. 37,922
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-7517

Enclosure: Notice of Appeal